HL7 EHR TC

Electronic Health Record-System Functional Model, Release 1 February 2007

Chapter Five: Information Infrastructure Functions

EHR Technical Committee Co-chairs:

Linda Fischetti, RN, MS
Veterans Health Administration

Don Mon
American Health Information Management Association

John Ritter
Intel Corporation

David Rowlands
Standards Australia

1 Example 2
2 Actors 2
3 Functional Outline 2
IN.1 (Security) 3
IN.1.1 (Entity Authentication) 3
IN.1.2 (Entity Authorization.) 4
IN.1.3 (Entity Access Control) 5
IN.1.4 (Patient Access Management) 6
IN.1.5 (Non-Repudiation) 6
IN.1.6 (Secure Data Exchange) 7
IN.1.7 (Secure Data Routing) 8
IN.1.8 (Information Attestation) 9
IN.1.9 (Patient Privacy and Confidentiality) 10
IN.2 (Health Record Information and Management) 10
IN.2.1 (Data Retention, Availability and Destruction) 11
IN.2.2 (Auditable Records) 12
IN.2.3 (Synchronization) 14
IN.2.4 (Extraction of Health Record Information) 14
IN.2.5 (Store and Manage Health Record Information) 15
IN.2.5.1 (Manage Unstructured Health Record Information) 16
IN.2.5.2 (Manage Structured Health Record Information) 17
IN.3 (Registry and Directory Services) 18
IN.4 (Standard Terminologies and Terminology Services) 19
IN.4.1 (Standard Terminologies and Terminology Models) 20
IN.4.2 (Maintenance and Versioning of Standard Terminologies) 21
IN.4.3 (Terminology Mapping) 22
IN.5 (Standards-based Interoperability) 23
IN.5.1 (Interchange Standards) 24
IN.5.2 (Interchange Standards Versioning and Maintenance) 26
IN.5.3 (Standards-based Application Integration) 28
IN.5.4 (Interchange Agreements) 29
IN.6 (Business Rules Management) 30
IN.7 (Workflow Management) 31

Chapter 5: Information Infrastructure EHR-S Functions

The Information Infrastructure section consists of common functions that support the Direct Care and Supportive Functions. Information Infrastructure functions are not involved in the provision of healthcare, but are necessary to ensure that the EHR-S provides necessary safeguards for patient safety, privacy and information security, as well as operational efficiencies and minimum standards for interoperability. They may be provided by the applications that support managing the health record, supporting infrastructure or a combination of both.

1 Example

For example, Direct Care and Supportive EHR-S functions must operate in a secure environment. Therefore, Information Infrastructure functions will provide a secure electronic environment for the immunization registration query mentioned previously and will report the child's immunization event in a secure manner. Information Infrastructure functions will also transparently provide other essential services, such as the archival and backup of the child's record and an audit trail of all accesses to the child's record.

2 Actors

The functions are expected to be performed transparently by EHR-S applications on behalf of EHR-S end-users. The System Administrator is expected to be involved in all operations related to configuring and managing the EHR-S operation. A security administrator is the person responsible for implementing security policy for authentication, authorization, and access control.

3 Functional Outline – Information Infrastructure

Information Infrastructure	IN.1	Security
	IN.2	Health Record Information and Management
	IN.3	Registry and Directory Services
	IN.4	Standard Terminologies & Terminology Services
	IN.5	Standards-based Interoperability
	IN.6	Business Rules Management
	IN.7	Workflow Management

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
IN.1	**H**	Security	**Statement:** Secure the access to an EHR-S and EHR information. Manage the sets of access control permissions granted within an EHR-S. Prevent unauthorized use of data, data loss, tampering and destruction. **Description:** To enforce security, all EHR-S applications must adhere to the rules established to control access and protect the privacy of EHR information. Security measures assist in preventing unauthorized use of data and protect against loss, tampering and destruction. An EHR-S must be capable of including or interfacing with standards-conformant security services to ensure that any Principal (user, organization, device, application, component, or object) accessing the system or its data is appropriately authenticated, authorized and audited in conformance with local and/or jurisdictional policies. An EHR-S should support Chains of Trust in respect of authentication, authorization, and privilege management, either intrinsically or by interfacing with relevant external services.			1
IN.1.1	**F**	Entity Authentication	**Statement:** Authenticate EHR-S users and/or entities before allowing access to an EHR-S. **Description:** Both users and applications are subject to authentication. The EHR-S must provide mechanisms for users and applications to be authenticated. Users will have to be authenticated when they attempt to use the application, the applications must authenticate		1. The system **SHALL** authenticate principals prior to accessing an EHR-S application or EHR-S data.	2
					2. The system **SHALL** prevent access to EHR-S applications or EHR-S data to all non-authenticated principals.	3

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			themselves before accessing EHR information managed by other applications or remote EHR-S'. In order for authentication to be established a Chain of Trust agreement is assumed to be in place. Examples of entity authentication include: - username/ password - digital certificate - secure token - biometrics		3. The system **SHOULD** provide the ability to implement a Chain of Trust agreement.	4
					4. IF other appropriate authentication mechanisms are absent, THEN the system SHALL authenticate principals using at least one of the following authentication mechanisms: username/password, digital certificate, secure token or biometrics.	5
IN.1.2	**F**	Entity Authorization.	**Statement:** Manage the sets of access-control permissions granted to entities that use an EHR-S (EHR-S Users). Enable EHR-S security administrators to grant authorizations to users, for roles, and within contexts. A combination of these authorization categories may be applied to control access to EHR-S functions or data within an EHR-S, including at the application or the operating system level. **Description:** EHR-S Users are authorized to use the components of an EHR-S according to their identity, role, work-assignment, location and/or the patient's present condition and the EHR-S User's scope of practice within a legal jurisdiction. - User based authorization refers to the permissions granted or denied based on the identity of an individual. An example of User based authorization is a patient defined denial of access to all or part of a record to a particular party for privacy related reasons. Another user based	IN.1.3 S.1.3.1	1. The system **SHALL** provide the ability to create and update sets of access-control permissions granted to principals.	6
					2. The system **SHALL** conform to function IN.2.2 (Auditable Records) for the purpose of recording all authorization actions.	7
					3. The system **SHALL** provide EHR-S security administrators with the ability to grant authorizations to principals according to scope of practice, organizational policy, or jurisdictional law.	8

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			authorization is for a tele-monitor device or robotic access to an EHR-S for prescribed directions and other input. - Role based authorization refers to the responsibility or function performed in a particular operation or process. Example roles include: an application or device (tele-monitor or robotic); or a nurse, dietician, administrator, legal guardian, and auditor. - Context-based Authorization is defined by ISO 10181-3 Technical Framework for Access Control Standard as security-relevant properties of the context in which an access request occurs, explicitly time, location, route of access, and quality of authentication. For example, an EHR-S might only allow supervising providers' context authorization to attest to entries proposed by residents under their supervision. In addition to the ISO standard, context authorization for an EHR-S is extended to satisfy special circumstances such as, work assignment, patient consents and authorizations, or other healthcare-related factors. A context-based example is a patient-granted authorization to a specific third party for a limited period to view specific EHR records. Another example is a right granted for a limited period to view those, and only those, EHR records connected to a specific topic of investigation.		4. The system **SHALL** provide EHR-S security administrators with the ability to grant authorizations for roles according to scope of practice, organizational policy, or jurisdictional law.	9
					5. The system **SHALL** provide EHR-S security administrators with the ability to grant authorizations within contexts according to scope of practice, organizational policy, or jurisdictional law.	10
					6. The system **MAY** provide the ability to define context for the purpose of principal authorization based on identity, role, work assignment, present condition, location, patient consent, or patient's present condition.	11
					7. The system **MAY** provide the ability to define context based on legal requirements or disaster conditions.	12
IN.1.3	**F**	Entity Access Control	**Statement:** Verify and enforce access control to all EHR-S components, EHR information and functions for end-users,		1. The system **SHALL** conform to function IN.1.1 (Entity Authentication).	13

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			applications, sites, etc., to prevent unauthorized use of a resource. **Description:** Entity Access Control is a fundamental function of an EHR-S. To ensure that access is controlled, an EHR-S must perform authentication and authorization of users or applications for any operation that requires it and enforce the system and information access rules that have been defined.		2. The system **SHALL** conform to function IN.1.2 (Entity Authorization).	14
					3. The system **SHALL** provide the ability to define system and data access rules.	15
					4. The system **SHALL** enforce system and data access rules for all EHR-S resources (at component, application, or user level, either local or remote).	16
IN.1.4	**F**	Patient Access Management	**Statement:** Enable a healthcare delivery organization to allow and manage a patient's access to the patient's personal health information. **Description:** A healthcare delivery organization will be able to manage a patient's ability to view his or her EHR based on scope of practice, organization policy or jurisdictional law. Typically, a patient has the right to view his or her EHR and the right to place restrictions on who can view parts or the whole of that EHR. For example, in some jurisdictions, minors have the right to restrict access to their data by parents/guardians. One example of managing a patient's access to his or her data is by extending user access controls to patients.		1. The system **SHALL** conform to function IN.1.3 (Entity Access Control) in order for a healthcare delivery organization to manage a patient's access to his or her healthcare information.	17
IN.1.5	**F**	Non-Repudiation	**Statement:** Limit an EHR-S user's ability to deny (repudiate) the origination, receipt, or authorization of a data exchange by that user. **Description:** An EHR-S allows data entry and data access to a patient's electronic health record and it can be a		1. The system **SHALL** time stamp initial entry, modification, or exchange of data, and identify the actor/principal taking the action as required by users' scope of practice, organizational policy, or jurisdictional law.	18

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			sender or receiver of healthcare information. Non repudiation guarantees that the source of the data record can not later deny that it is the source; that the sender or receiver of a message cannot later deny having sent or received the message. For example, non-repudiation may be achieved through the use of a: - Digital signature, which serves as a unique identifier for an individual (much like a written signature on a paper document). - Confirmation service, which utilizes a message transfer agent to create a digital receipt (providing confirmation that a message was sent and/or received) and - Timestamp, which proves that a document existed at a certain date and time. Date and Time stamping implies the ability to indicate the time zone where it was recorded (time zones are described in ISO 8601 Standard Time Reference).		2. The system **SHALL** provide additional non-repudiation functionality where required by users' scope of practice, organizational policy, or jurisdictional law.	19
					3. The system **MAY** conform to function IN.2.2 (Auditable Records) to prevent repudiation of data origination, receipt, or access.	20
					4. The system **MAY** conform to function IN.1.8 (Information Attestation) to ensure the integrity of data exchange and thus prevent repudiation of data origination or receipt.	21
IN.1.6	**F**	Secure Data Exchange	**Statement:** Secure all modes of EHR data exchange. **Description:** Whenever an exchange of EHR information occurs, it requires appropriate security and privacy considerations, including data obfuscation as well as both destination and source authentication when necessary. For example, it may be necessary to encrypt data sent to remote or external destinations. A secure data exchange requires that there is an overall coordination regarding the information that is exchanged between EHR-S entities and how that exchange is expected to occur. The policies applied at	IN.1.1 IN.2.2	1. The system **SHALL** secure all modes of EHR data exchange.	22
					2. The system **SHOULD** conform to function IN.1.7 (Secure Data Routing).	23
					3. The system **MAY** provide the ability to obfuscate data.	24
					4. The system **SHALL** encrypt and decrypt EHR data that is exchanged over a non-secure link.	25

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			different locations must be consistent or compatible with each other in order to ensure that the information is protected when it crosses entity boundaries within an EHR-S or external to an EHR-S.		5. The system **SHALL** support standards-based encryption mechanisms when encryption is used for secure data exchange.	26
IN.1.7	**F**	Secure Data Routing	**Statement:** Route electronically exchanged EHR data only to/from known, registered, and authenticated destinations/sources (according to applicable healthcare-specific rules and relevant standards). **Description:** An EHR-S needs to ensure that it is exchanging EHR information with the entities (applications, institutions, directories) it expects. This function depends on entity authorization and authentication to be available in the system. For example, a physician practice management application in an EHR-S might send claim attachment information to an external entity. To accomplish this, the application must use a secure routing method, which ensures that both the sender and receiving sides are authorized to engage in the information exchange. Known sources and destinations can be established in a static setup or they can be dynamically determined. Examples of a static setup are recordings of IP addresses or recordings of DNS names. For dynamic determination of known	IN.1.1 IN.1.2	1. The system **SHALL** automatically route electronically exchanged EHR data only from and to known sources and destinations and only over secure networks.	27
					2. The system **SHOULD** route electronically exchanged EHR data only to and from authenticated sources and destinations (conform to function IN.1.1 (Entity Authentication)).	28

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			sources and destinations systems can use authentication mechanisms as described in IN.1.1. For example, the sending of a lab order from the EHRS to a lab system within the same organization usually uses a simple static setup for routing. In contrast sending a lab order to a reference lab outside of the organization will involve some kind of authentication process. In general, when the underlying network infrastructure is secure (e.g. secure LAN or VPN) the simple static setup is used.		3. The system **SHOULD** conform to function IN.2.2 (Auditable Records) to provide audit information about additions and changes to the status of destinations and sources.	29
IN.1.8	**F**	Information Attestation	**Statement:** Manage electronic attestation of information including the retention of the signature of attestation (or certificate of authenticity) associated with incoming or outgoing information. **Description:** The purpose of attestation is to show authorship and assign responsibility for an act, event, condition, opinion, or diagnosis. Every entry in the health record must be identified with the author and should not be made or signed by someone other than the author. (Note: A transcriptionist may transcribe an author's notes and a senior clinician may attest to the accuracy of another's statement of events.) Attestation is required for (paper or electronic) entries such as narrative or progress notes, assessments, flow sheets, and orders. Digital signatures may be used to implement document attestation. For an incoming document, the record of attestation is retained if included. Attestation functionality must meet applicable legal, regulatory and other applicable standards or requirements.		1. The system **SHALL** conform to function IN.1.1 (Entity Authentication).	30
					2. The system **SHALL** conform to function IN.1.2 (Entity Authorization).	31
					3. The system **SHALL** provide the ability to associate any attestable content added or changed to an EHR with the content's author (for example by conforming to function IN.2.2 (Auditable Records).	32
					4. The system **SHALL** provide the ability for attestation of attestable EHR content by the content's author.	33
					5. The system **SHALL** indicate the status of attestable data which has not been attested.	34
					6. The system **MAY** provide the ability for attestation of EHR content by properly authenticated and authorized users different from the author as required by users' scope of practice, organizational policy, or jurisdictional law.	35
					7. The system **MAY** provide the ability to use digital signatures as the means for attestation.	36

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
IN.1.9	**F**	Patient Privacy and Confidentiality	**Statement:** Enable the enforcement of the applicable jurisdictional and organizational patient privacy rules as they apply to various parts of an EHR-S through the implementation of security mechanisms. **Description:** Patients' privacy and the confidentiality of EHRs are violated if access to EHRs occurs without authorization. Violations or potential violations can impose tangible economic or social losses on affected patients, as well as less tangible feelings of vulnerability and pain. Fear of potential violations discourages patients from revealing sensitive personal information that may be relevant to diagnostic and treatment services. Rules for the protection of privacy and confidentiality may vary depending upon the vulnerability of patients and the sensitivity of records. Strongest protections should apply to the records of minors and the records of patients with stigmatized conditions. Authorization to access the most sensitive parts of an EHR is most definitive if made by the explicit and specific consent of the patient. Please see the definition of masking in the glossary.	IN.6	1. The system **SHALL** provide the ability to fully comply with the requirements for patient privacy and confidentiality in accordance with a user's scope of practice, organizational policy, or jurisdictional law.	37
					2. The system **SHALL** conform to function IN.1.1 (Entity Authentication).	38
					3. The system **SHALL** conform to function IN.1.2 (Entity Authorization).	39
					4. The system **SHALL** conform to function IN.1.3 (Entity Access Control).	40
					5. The system **SHOULD** conform to function IN.1.5 (Non-Repudiation).	41
					6. The system **SHOULD** conform to function IN.1.6 (Secure Data Exchange).	42
					7. The system **SHOULD** conform to function IN.2.2 (Auditable Records).	43
					8. The system **SHALL** provide the ability to maintain varying levels of confidentiality in accordance with users' scope of practice, organizational policy, or jurisdictional law.	44
					9. The system **SHALL** provide the ability to mask parts of the electronic health record (e.g. medications, conditions, sensitive documents) from disclosure according to scope of practice, organizational policy or jurisdictional law.	45
					10. The system **SHALL** provide the ability to override a mask in emergency or other specific situations according to scope of practice, organizational policy or jurisdictional law.	46
IN.2	**H**	Health Record Information and Management	**Statement:** Manage EHR information across EHR-S applications by ensuring that clinical information entered by providers is a valid representation of clinical notes; and is accurate and complete according to clinical rules and tracking amendments to clinical documents. Ensure that information entered by or on behalf of the patient is			47

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			accurately represented. **Description:** Since EHR information will typically be available on a variety of EHR-S applications, an EHR-S must provide the ability to access, manage and verify accuracy and completeness of EHR information, maintain the integrity and reliability of the data, and provide the ability to audit the use of and access to EHR information.			
IN.2.1	**F**	Data Retention, Availability and Destruction	**Statement:** Retain, ensure availability, and destroy health record information according to scope of practice, organizational policy, or jurisdictional law. This includes: -Retaining all EHR-S data and clinical documents for the time period designated by policy or legal requirement; -Retaining inbound documents as originally received (unaltered); -Ensuring availability of information for the legally prescribed period of time to users and patients; and -Providing the ability to destroy EHR data/records in a systematic way according to policy and after the legally prescribed retention period. **Description:** Discrete and structured EHR-S data, records and reports must be: -Made available to users in a timely fashion; -Stored and retrieved in a semantically intelligent and useful manner (for example, chronologically, retrospectively per a given disease or event, or in accordance with business requirements, local policies, or legal requirements); -Retained for a legally prescribed period of time; and -Destroyed in a systematic manner in relation to the applicable retention period.	IN.1.7	1. The system **SHALL** provide the ability to store and retrieve health record data and clinical documents for the legally prescribed time.	48
					2. The system **SHALL** provide the ability to retain inbound data or documents (related to health records) as originally received (unaltered, inclusive of the method in which they were received) for the legally organizationally prescribed time in accordance with users' scope of practice, organizational policy, or jurisdictional law.	49
					3. The system **SHALL** retain the content of inbound data (related to health records) as originally received for the legally prescribed time.	50
					4. The system **SHOULD** provide the ability to retrieve both the information and business context data within which that information was obtained.	51
					5. The system **SHOULD** provide the ability to retrieve all the elements included in the definition of a legal medical record.	52
					6. The system **MAY** provide the ability to identify specific EHR data/records for destruction, review and confirm destruction before it occurs and implement function IN.2.2 (Auditable Records).	53

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			An EHR-S must also allow an organization to identify data/records to be destroyed, and to review and approve destruction before it occurs. In such a case it should pass along record destruction date information along with existing data when providing records to another entity.		7. The system **MAY** provide the ability to destroy EHR data/records so that all traces are irrecoverably removed according to policy and legal retentions periods.	54
					8. The system **SHOULD** pass along record destruction date information (if any) along with existing data when providing records to another entity.	55
IN.2.2	**F**	Auditable Records	**Statement:** Provide audit capabilities for system access and usage indicating the author, the modification (where pertinent), and the date and time at which a record was created, modified, viewed, extracted, or deleted. Date and Time stamping implies the ability to indicate the time zone where it was recorded (time zones are described in ISO 8601 Standard Time Reference). Auditable records extend to information exchange, to audit of consent status management (to support DC.1.3.3) and to entity authentication attempts. Audit functionality includes the ability to generate audit reports and to interactively view change history for individual health records or for an EHR-S. **Description:** Audit functionality extends to security audits, data audits, audits of data exchange, and the ability to generate audit reports. Audit capability settings should be configurable to meet the needs of local policies. Examples of audited areas include: - Security audit, which logs access attempts and resource usage including user login, file access, other various activities, and whether any actual or attempted security violations occurred		1. The system **SHALL** provide audit capabilities for recording access and usage of systems, data, and organizational resources.	56
					2. The system **SHALL** conform to function IN.1.1 (Entity Authentication).	57
					3. The system **SHALL** provide audit capabilities indicating the time stamp for an object or data creation.	58
					4. The system **SHALL** provide audit capabilities indicating the time stamp for an object or data modification in accordance with users' scope of practice, organizational policy, or jurisdictional law.	59
					5. The system **SHALL** provide audit capabilities indicating the time stamp for an object or data extraction in accordance with users' scope of practice, organizational policy, or jurisdictional law.	60
					6. The system **SHALL** provide audit capabilities indicating the time stamp for an object or data exchange.	61
					7. The system **SHOULD** provide audit capabilities indicating the time stamp for an object or data view.	62
					8. The system **SHALL** provide audit capabilities indicating the time stamp for an object or data deletion in accordance with users' scope of practice, organizational policy, or jurisdictional law.	63
					9. The system **SHALL** provide audit capabilities indicating the author of a change in accordance with users' scope of practice, organizational policy, or jurisdictional law.	64

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			- Data audit, which records who, when, and by which system an EHR record was created, updated, translated, viewed, extracted, or (if local policy permits) deleted. Audit-data may refer to system setup data or to clinical and patient management data - Information exchange audit, which records data exchanges between EHR-S applications (for example, sending application; the nature, history, and content of the information exchanged); and information about data transformations (for example, vocabulary translations, reception event details, etc.) - Audit reports should be flexible and address various users' needs. For example, a legal authority may want to know how many patients a given healthcare provider treated while the provider's license was suspended. Similarly, in some cases a report detailing all those who modified or viewed a certain patient record - Security audit trails and data audit trails are used to verify enforcement of business, data integrity, security, and access-control rules -There is a requirement for system audit trails for the following events: >Loading new versions of, or changes to, the clinical system; >Loading new versions of codes and knowledge bases; >Taking and restoring of backup; >Changing the date and time where the		10. The system **SHOULD** provide audit capabilities indicating the viewer of a data set.	65
					11. The system **MAY** provide audit capabilities indicating the data value before a change.	66
					12. The system **MAY** provide audit capabilities to capture system events at the hardware and software architecture level.	67
					13. The system **SHALL** conform to function IN.1.3 (Entity Access Control) to limit access to audit record information to appropriate entities in accordance with users' scope of practice, organizational policy, or jurisdictional law.	68
					14. The system **SHALL** provide the ability to generate an audit report.	69
					15. The system **SHALL** provide the ability to view change history for a particular record or data set in accordance with users' scope of practice, organizational policy, or jurisdictional law.	70
					16. The system **SHOULD** provide the ability to record system maintenance events for loading new versions of, or changes to, the clinical system.	71
					17. The system **SHOULD** provide the ability to record system maintenance events for loading new versions of codes and knowledge bases.	72
					18. The system **SHOULD** provide the ability to record changing the date and time where the clinical system allows this to be done.	73
					19. The system **SHOULD** provide the ability to record system maintenance events for creating and restoring of backup.	74
					20. The system **SHOULD** provide the ability to record system maintenance events for archiving any data.	75
					21. The system **SHOULD** provide the ability to record system maintenance events for re-activating of an archived patient record.	76

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			clinical system allows this to be done; >Archiving any data; >Re-activating of an archived patient record; >Entry to and exiting from the clinical system; >Remote access connections including those for system support and maintenance activities		22. The system **SHOULD** provide the ability to record system maintenance events for entry to and exit from the EHR system.	77
					23. The system **SHOULD** provide the ability to record system maintenance events for remote access connections including those for system support and maintenance activities**.**	78
					24. The system **SHOULD** utilize standardized time keeping (for example using the IHE consistent time profile).	79
					25. The system **SHOULD** provide the ability to record and report upon audit information using a standards-based audit record format (for example RFC 3881).	80
IN.2.3	**F**	Synchronization	**Statement:** Maintain synchronization involving: -Interaction with entity directories; -Linkage of received data with existing entity records; -Location of each health record component; and -Communication of changes between key systems. **Description:** An EHR-S may consist of a set of components or applications; each application manages a subset of the health information. Therefore it is important that, through various interoperability mechanisms, an EHR-S maintains all the relevant information regarding the health record in synchrony. For example, if a physician orders an MRI, a set of diagnostic images and a radiology report will be created. The patient demographics, the order for MRI, the diagnostic images associated with the order, and the report associated with the study must all be synchronized in order for the clinicians to view the complete record.		1. The system **SHALL** conform to function IN.5.1 (Interchange Standards).	81
					2. The system **SHOULD** conform to function IN.3 (Registry and Directory Services) to enable the use of registries and directories.	82
					3. The system **SHOULD** provide the ability to link entities to external information.	83
					4. The system **SHOULD** store the location of each known health record component in order to enable authorized access to a complete logical health record if the EHR is distributed among several applications within the EHR-S.	84
IN.2.4	**F**	Extraction of Health Record Information	**Statement:** Manage data extraction in accordance with analysis and reporting	S.2.2	1. The system **SHALL** provide the ability to extract health record information.	85

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			requirements. The extracted data may require use of more than one application and it may be pre-processed (for example, by being de-identified) before transmission. Data extractions may be used to exchange data and provide reports for primary and ancillary purposes. **Description:** An EHR-S enables an authorized user, such as a clinician, to access and aggregate the distributed information, which corresponds to the health record or records that are needed for viewing, reporting, disclosure, etc. An EHR-S must support data extraction operations across the complete data set that constitutes the health record of an individual and provide an output that fully chronicles the healthcare process. Data extractions are used as input to patient care coordination between facilities, organizations and settings. In addition, data extractions can be used for administrative, financial, research, quality analysis, and public health purposes.		2. The system **SHOULD** conform to function IN.1.6 (Secure Data Exchange) to provide secure data exchange capabilities.	86
					3. The system **SHOULD** provide the ability to de-identify extracted information.	87
					4. The system **SHOULD** conform to function IN.5.1 (Interchange Standards) to enable data extraction in standard-based formats.	88
					5. The system **SHOULD** provide the ability to perform extraction operations across the complete data set that constitutes the health record of an individual within the system.	89
					6. The system **MAY** provide the ability to perform extraction operations whose output fully chronicles the healthcare process.	90
					7. The system **SHOULD** provide the ability to extract data for administrative purposes.	91
					8. The system **SHOULD** provide the ability to extract data for financial purposes.	92
					9. The system **SHOULD** provide the ability to extract data for research purposes.	93
					10. The system **SHOULD** provide the ability to extract data for quality analysis purposes.	94
					11. The system **SHOULD** provide the ability to extract data for public health purposes.	95
IN.2.5	**H**	Store and Manage Health Record Information	**Statement:** Store and manage health record information as structured and unstructured data **Description:** Unstructured health record information is information that is not divided into discrete fields AND not represented as numeric, enumerated or codified data. General examples of unstructured health record information include: - text - word processing document - image			96

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			- multimedia Specific examples include: - text message to physician - patient photo - letter from family - scanned image of insurance card - dictated report (voice recording) Structured health record information is divided into discrete fields, and may be enumerated, numeric or codified. Examples of structured health information include: - patient address (non-codified, but discrete field) - diastolic blood pressure (numeric) - coded result observation - coded diagnosis - patient risk assessment questionnaire with multiple-choice answers Context may determine whether or not data are unstructured, e.g., a progress note might be standardized and structured in some EHR-S (e.g., Subjective/Objective/Assessment/Plan) but unstructured in others. Managing healthcare data includes capture, retrieval, deletion, correction, amendment, and augmentation. Augmentation refers to providing additional information regarding the healthcare data, which is not part of the data itself, e.g. linking patient consents or authorizations to the healthcare data of the patient.			
IN.2.5.1	**F**	Manage Unstructured Health Record Information	**Statement:** Create, capture, and maintain unstructured health record information.		1. The system **SHALL** capture unstructured health record information as part of the patient EHR. 2. The system **SHALL** retrieve unstructured health record	97 98

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			Description:		information as part of the patient EHR.	
					3. The system **SHALL** provide the ability to update unstructured health record information.	99
					4. The system **SHALL** conform to function IN.2.1 (Data Retention, Availability and Destruction) to provide the ability to inactivate, obsolete, or destroy unstructured health record information.	100
					5. The system **SHOULD** provide the ability to report unstructured health record information.	101
					6. The system **MAY** track unstructured health record information over time.	102
					7. The system **SHALL** provide the ability to append corrected unstructured health record information to the original unstructured health record information. A specific type of implementation is not implied.	103
					8. The system **SHALL** provide the ability to append unstructured health record information to the original unstructured health record information. A specific type of implementation is not implied.	104
					9. The system **SHALL** provide the ability to append augmented unstructured health record information to the original unstructured health record information. A specific type of implementation is not implied.	105
IN.2.5.2	**F**	Manage Structured Health Record Information	**Statement:** Create, capture, and maintain structured health record information. **Description:** Structured health record information is divided into discrete fields, and may be enumerated, numeric or codified. Examples of structured health information include: - patient address (non-codified, but discrete field) - diastolic blood pressure (numeric) - coded result observation - coded diagnosis - patient risk assessment questionnaire with multiple-choice answers Context may determine whether or not		1. The system **SHALL** capture structured health record information as part of the patient EHR.	106
					2. The system **SHALL** retrieve structured health record information as part of the patient EHR.	107
					3. The system **SHALL** provide the ability to update structured health record information.	108
					4. The system **SHALL** conform to function IN.2.1 (Data Retention, Availability and Destruction) to provide the ability to inactivate, obsolete, or destroy structured health record information.	109
					5. The system **SHOULD** provide the ability to report structured health record information.	110
					6. The system **MAY** track structured health record information over time.	111
					7. The system **SHOULD** provide the ability to retrieve each item of structured health record information discretely	112

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			Context may determine whether or not data are unstructured, e.g., a progress note might be standardized and structured in some EHRS (e.g., Subjective/Objective/Assessment/Plan) but unstructured in others.		within patient context.	
					8. The system **SHALL** provide the ability to append corrected structured health record information to the original structured health record information. A specific type of implementation is not implied.	113
					9. The system **SHALL** provide the ability to append structured health record information to the original structured health record information. A specific type of implementation is not implied.	114
					10. The system **SHALL** provide the ability to append augmented structured health record information to the original structured health record information. A specific type of implementation is not implied.	115
IN.3	**F**	Registry and Directory Services	**Statement:** Enable the use of registry services and directories to uniquely identify, locate and supply links for retrieval of information related to: - patients and providers for healthcare purposes; - payers, health plans, sponsors, and employers for administrative and financial purposes; - public health agencies for healthcare purposes, and - healthcare resources and devices for resource management purposes. **Description:** Registry and directory service functions are critical to successfully managing the security, interoperability, and the consistency of the health record data across an EHR-S. These services enable the linking of relevant information across multiple information sources within, or external to, an EHR-S for use within an application. Directories and registries support communication between EHR Systems and may be organized hierarchically or in a federated fashion. For example, a		1. The system **SHALL** provide the ability to use registry services and directories.	116
					2. The system **SHOULD** provide the ability to securely use registry services and directories.	117
					3. The system **SHALL** conform to function IN.5.1 (Interchange Standards) to provide standard data interchange capabilities for using registry services and directories.	118
					4. The system **SHOULD** communicate with local registry services through standardized interfaces.	119
					5. The system **SHOULD** communicate with non-local registry services (that is, to registry services that are external to an EHR-S) through standardized interfaces.	120
					6. The system **SHOULD** provide the ability to use registries or directories to uniquely identify patients for the provision of care.	121
					7. The system **SHOULD** provide the ability to use registries or directories to uniquely identify providers for the provision of care.	122
					8. The system **MAY** provide the ability to use registries or directories to retrieve links to relevant healthcare information regarding a patient.	123

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			patient being treated by a primary care physician for a chronic condition may become ill while out of town. The new provider's EHR-S interrogates a local, regional, or national registry to find the patient's previous records. From the primary care record, a remote EHR-S retrieves relevant information in conformance with applicable patient privacy and confidentiality rules. An example of local registry usage is an EHR-S application sending a query message to the Hospital Information System to retrieve a patient's demographic data.		9. The system **MAY** provide the ability to use registries to supply links to relevant healthcare information regarding a patient.	124
					10. The system **MAY** provide the ability to use registries or directories to identify payers, health plans, and sponsors for administrative and financial purposes.	125
					11. The system **MAY** provide the ability to use registries or directories to identify employers for administrative and financial purposes.	126
					12. The system **MAY** provide the ability to use registries or directories to identify public health agencies for healthcare purposes.	127
					13. The system **MAY** provide the ability to use registries or directories to identify healthcare resources and devices for resource management purposes.	128
IN.4	**H**	Standard Terminologies and Terminology Services	**Statement:** Support semantic interoperability through the use of standard terminologies, standard terminology models and standard terminology services. **Description:** The purpose of supporting terminology standards and services is to enable semantic interoperability. Interoperability is demonstrated by the consistency of human and machine interpretation of shared data and reports. It includes the capture and support of consistent data for templates and decision support logic. Terminology standards pertain to concepts, representations, synonyms, relationships and computable (machine-readable) definitions. Terminology services provide a common way for managing and retrieving these items.			129

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
IN.4.1	**F**	Standard Terminologies and Terminology Models	**Statement:** Employ standard terminologies to ensure data correctness and to enable semantic interoperability (both within an enterprise and externally). Support a formal standard terminology model. **Description:** Semantic interoperability requires standard terminologies combined with a formal standard information model. An example of an information model is the HL7 Reference Information model. Examples of terminologies that an EHR-S may support include: LOINC, SNOMED, ICD-9, ICD-10, and CPT-4. A terminology provides semantic and computable identity to its concepts. Terminologies are use-case dependent and may or may not be realm dependent. For example, terminologies for public health interoperability may differ from those for healthcare quality, administrative reporting, research, etc. Formal standard terminology models enable common semantic representations by describing relationships that exist between concepts within a terminology or in different terminologies, such as exemplified in the model descriptions contained in the HL7 Common Terminology Services specification. The clinical use of standard terminologies		1. The system **SHALL** provide the ability to use standard terminologies to communicate with other systems(internal or external to the EHR-S).	130
					2. The system **SHALL** provide the ability to validate that clinical terms and coded clinical data exists in a current standard terminology.	131
					3. The system **SHOULD** provide the ability to exchange healthcare data using formal standard information models and standard terminologies.	132
					4. The system **SHOULD** provide the ability to use a formal standard terminology model.	133

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			is greatly enhanced with the ability to perform hierarchical inference searches across coded concepts. Hierarchical Inference enables searches to be conducted across sets of coded concepts stored in an EHR-S. Relationships between concepts in the terminology are used in the search to recognize child concepts of a common parent. For example, there may be a parent concept, "penicillin containing preparations" which has numerous child concepts, each of which represents a preparation containing a specific form of penicillin (Penicillin V, Penicillin G, etc). Therefore, a search may be conducted to find all patients taking any form of penicillin preparation. Clinical and other terminologies may be provided through a terminology service internal or external to an EHR-S. An example of a terminology service is described in the HL7 Common Terminology Services specification.		5. The system **SHOULD** provide the ability to use hierarchical inference searches e.g., subsumption across coded terminology concepts that were expressed using standard terminology models.	134
					6. The system **SHOULD** provide the ability to use a terminology service (internal or external to the EHR-S).	135
					7. IF there is no standard terminology model available, THEN the system **MAY** provide a formal explicit terminology model.	136
IN.4.2	**F**	Maintenance and Versioning of Standard Terminologies	**Statement:** Enable version control according to customized policies to ensure maintenance of utilized standards. This includes the ability to accommodate changes to terminology sets as the source terminology undergoes its natural update process (new codes, retired codes, redirected codes). Such changes need to be cascaded to clinical content embedded in templates, custom formularies, etc., as determined by local policy. **Description:** Version control allows for multiple sets or versions of the same		1. The system **SHALL** provide the ability to use different versions of terminology standards.	137
					2. The system **SHALL** provide the ability to update terminology standards.	138
					3. The system **MAY** relate modified concepts in the different versions of a terminology standard to allow preservation of interpretations over time.	139

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			terminology to exist and be distinctly recognized over time. Terminology standards are usually periodically updated, and concurrent use of different versions may be required. Since the meaning of a concept can change over time, it is important that retrospective analysis and research maintains the ability to relate changing conceptual meanings. If the terminology encoding for a concept changes over time, it is also important that retrospective analysis and research can correlate the different encodings to ensure the permanence of the concept. This does not necessarily imply that complete older versions of the terminology be kept in the EHR-S, only access to the changes needs to be maintained. It should be possible to retire deprecated versions when applicable business cycles are completed while maintaining obsolescent code sets. An example use of this is for possible claims adjustment throughout the claim's lifecycle.		4. The system **SHOULD** provide the ability to interoperate with systems that use known different versions of a terminology standard.	140
					5. The system **SHOULD** provide the ability to deprecate terminologies.	141
					6. The system **MAY** provide the ability to deprecate individual codes within a terminology.	142
					7. The system **SHALL** provide the ability to cascade terminology changes where coded terminology content is embedded in clinical models (for example, templates and custom formularies) when the cascaded terminology changes can be accomplished unambiguously.	143
					8. Changes in terminology **SHALL** be applied to all new clinical content (via templates, custom formularies, etc.).	144
IN.4.3	**F**	Terminology Mapping	**Statement:** Map or translate one terminology to another as needed by local, regional, national, or international interoperability requirements **Description:** The ability to map or translate one terminology to another is fundamental to an organization in an environment where several terminologies are in play with overlapping concepts. It is a common occurrence that data is captured using one terminology, but is shared using another terminology. For		1. The system **SHALL** provide the ability to use a terminology map.	145
					2. The system **SHOULD** provide the ability to use standard terminology services for the purposes of mapping terminologies.	146

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			example, within a healthcare organization there may be a need to map overlapping terminology concepts (e.g. between an EHRS and an external laboratory system, ore between an EHRS and a billing system). Realm specific (including local, regional, national or international) interoperability requirements can also determine the need for terminology mapping, and in many cases terminology mapping services can be used to satisfy these requirements.		3. The system **MAY** provide the ability for a user to validate a mapping.	147
					4. The system **MAY** provide the ability to create a terminology map.	148
IN.5	**H**	Standards-based Interoperability	**Statement:** Provide automated health care delivery processes and seamless exchange of clinical, administrative, and financial information through standards-based solutions. **Description:** Interoperability standards enable an EHR-S to operate as a set of applications. This results in a unified view of the system where the reality is that several disparate systems may be coming together. Interoperability standards also enable the sharing of information between EHR systems, including the participation in regional, national, or international information exchanges. Timely and efficient access to information and capture of information is promoted with minimal impact to the user.			149

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
IN.5.1	F	Interchange Standards	**Statement:** Support the ability to operate seamlessly with other systems, either internal or external, that adhere to recognized interchange standards. "Other systems" include other EHR Systems, applications within an EHR-S, or other authorized entities that interact with an EHR-S. **Description:** An organization typically uses a number of interchange standards to meet its external and internal interoperability requirements. It is fundamental that there be a common understanding of rules regarding connectivity, information structures, formats and semantics. These are known as "interoperability or interchange standards". Data exchange which may be between internal systems or modules, or external to the organization, is to occur in a manner which is seamless to the user. For example, if data interchange involves double entry, or manual cut-and-paste steps by the user, it is not considered seamless. Representation of EHR content is transmitted in a variety of interchange formats such as: HL7 Messages, Clinical Document Architecture (CDA) and other		1. The system **SHALL** provide the ability to use interchange standards as required by realm specific and/or local profiles.	150
					2. The system **SHALL** provide the ability to seamlessly perform interchange operations with other systems that adhere to recognized interchange standards.	151

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			HL7 Structured Documents, X12N healthcare transactions, and Digital Imaging and Communication in Medicine (DICOM) format. Support for multiple interaction modes is needed to respond to differing levels of immediacy and types of exchange. For example, messaging is effective for many near-real time, asynchronous data exchange scenarios but may not be appropriate if the end-user is requesting an immediate response from a remote application.		3. The system **SHALL** conform to functions under header IN.4 (Standard Terminologies and Terminology Services) to support terminology standards in accordance with a users' scope of practice, organizational policy, or jurisdictional law.	152
			A variety of interaction modes are typically supported such as: -Unsolicited Notifications, e.g. a patient has arrived for a clinic appointment -Query/Response e.g., Is Adam Everyman known to the system? Yes, MRN is 12345678. -Service Request and Response, e.g., Laboratory Order for "Fasting Blood Sugar" and a response containing the results of the test. -Information Interchange between organizations (e.g. in a RHIO, or in a		4. IF there is no standard information model available, THEN the system **MAY** provide a formal explicit information model in order to support the ability to operate seamlessly with other systems.	153

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			National Health System) -Structured/discrete clinical documents, e.g., Clinical Note -Unstructured clinical document, e.g., dictated surgical note Standard terminology is a fundamental part of interoperability and is described in section IN.4. Using a formal explicit information model further optimizes interoperability. An example of an information model is the HL7 Reference Information Model (RIM). Organizations typically need to deal with more than one information model and may need to develop a mapping or a meta-model.		5. The system **SHOULD** provide the ability to exchange data using an explicit and formal information model and standard, coded terminology.	154
IN.5.2	**F**	Interchange Standards Versioning and Maintenance	**Statement:** Enable version control according to local policies to ensure maintenance of utilized interchange standards. Version control of an interchange standard implementation includes the ability to accommodate changes as the source interchange standard undergoes its natural update process. **Description:** The life cycle of any given standard results in changes to its requirements. It is critical that an organization know the version of any given standard it uses and what its requirements and capabilities are. For example, if the organization migrates to an HL7 v2.5 messaging standard, it may choose to take advantage of new capabilities such as specimen or blood bank information. The organization may		1. The system **SHALL** provide the ability to use different versions of interchange standards.	155

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			find that certain fields have been retained for backwards compatibility only or withdrawn altogether. The EHR-S needs to be able to handle all of these possibilities. Standards typically evolve in such a way as to protect backwards compatibility. On the other hand, sometimes there is little, or no, backwards compatibility when an organization may need to replace an entire standard with a new methodology. An example of this is migrating from HL7 v2 to HL7 v3. Interchange standards that are backward compatible support exchange among senders and receivers who are using different versions. Version control ensures that those sending information in a later version of a standard consider the difference in information content that can be interchanged effectively with receivers, who are capable of processing only earlier versions. That is, senders need to be aware of the information that receivers are unable to capture and adjust their business processes accordingly. Version control enables multiple versions of the same interchange standard to exist and be distinctly recognized over time. Since interchange standards are usually periodically updated, concurrent use of different versions may be required. Large (and/or federated) organizations typically need to use different versions of an interchange standard to meet internal organizational interoperability requirements. For example, the enterprise-wide standard might use HL7 v2.5 for Lab messages, but some regions of the		2. The system **SHALL** provide the ability to change (reconfigure) the way that data is transmitted as an interchange standard evolves over time and in accordance with business needs.	156
					3. The system **SHOULD** provide the ability to deprecate an interchange standard.	157

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			enterprise might be at a lower level. It should be possible to retire deprecated interchange standards versions when applicable business cycles are completed while maintaining obsolete versions. An example use of this is for possible claims adjustment throughout the claim's life cycle. When interchange standards change over time, it is important that retrospective analysis and research correlate and note gaps between the different versions' information structures to support the permanence of concepts over time. An example use of this is the calculation of outcome or performance measures from persisted data stores where one version of a relevant interchange standard, e.g., CDA Release 1 captures the relevant data, e.g., discharge data, differently than CDA Release 2.		4. The system **SHOULD** provide the ability to interoperate with other systems that use known earlier versions of an interoperability standard.	158
IN.5.3	**F**	Standards-based Application Integration	**Statement:** Enable standards-based application integration with other systems. **Description:** When an organization wishes to integrate its applications, they must use standardized methods. Standards-based application integration may be achieved in a variety of ways. For example: -desktop visual integration may be achieved via HL7 Clinical Context Object Workgroup (CCOW) standards -workflow functions may be integrated via The Workflow Management Coalition (WfMC) standards -EHRS may be integrated in an Enterprise Information System Architecture via Service Oriented Architecture (SOA) standards It is recognized that these examples are		1. The system **SHALL** provide the ability to support standards-based application integration.	159

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			very disparate and used for very different purposes. The method used depends on the organization's approach to application integration. An organization could conceivably use multiple integration approaches.			
IN.5.4	**F**	Interchange Agreements	**Statement:** Support interactions with entity directories to determine the address, profile and data exchange requirements of known and/or potential partners. Use the rules of interaction specified in the partner's interchange agreement when exchanging information. **Description:** Systems that wish to communicate with each other, must agree on the parameters associated with that information exchange. Interchange Agreements allow an EHR-S to describe those parameters/criteria. An EHR-S can use the entity registries to determine the security, addressing, and reliability requirements between partners. An EHR-S can use this information to define how data will be exchanged between the sender and the receiver. Discovery of interchange services and capabilities can be automatic. For example: - A new application can automatically determine a patient demographics source using ~~a~~ Universal Description and Discovery Integration (UDDI) for source discovery, and retrieve the Web Services Description Language (WSDL) specification for binding details.	IN.3	1. The system **SHALL** use interchange agreement descriptions when exchanging information with partners**.**	160
					2. The system **SHOULD** use interchange agreement description standards (when available).	161
					3. The system **MAY** conform to function IN.3 (Registry and Directory Services) to interact with entity directories to determine the address, profile and data exchange requirements of known and/or potential partners.	162

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			- Good Health Hospital is a member of AnyCounty LabNet, for sharing laboratory results with other partners. Good Health Hospital periodically queries LabNet's directory (UDDI) to determine if additional information providers have joined LabNet. When new information providers are discovered, the Good Health IT establishes the appropriate service connections based upon the Service Description (WSDL).		4. The system **MAY** provide the ability to automatically discover interchange services and capabilities.	163
IN.6	**F**	Business Rules Management	**Statement:** Manage the ability to create, update, delete, view, and version business rules including institutional preferences. Apply business rules from necessary points within an EHR-S to control system behavior. An EHR-S audits changes made to business rules, as well as compliance to and overrides of applied business rules. **Description:** EHR-S business rule implementation functions include: decision support, diagnostic support, workflow control, and access privileges, as well as system and user defaults and preferences. An EHR-S supports the ability of providers and institutions to customize decision support components such as triggers, rules, or algorithms, as well as the wording of alerts and advice to meet realm specific requirements and preferences. Examples of applied business rules include: - Suggesting diagnosis based on the combination of symptoms (flu-like symptoms combined with widened mediastinum suggesting anthrax);	DC.2.2 S.3.1 S.3.7	1. The system **SHALL** provide the ability to manage business rules.	164
					2. The system **SHOULD** provide the ability to create, import, or access decision support rules to guide system behavior.	165
					3. The system **SHOULD** provide the ability to update decision support rules.	166
					4. The system **SHOULD** provide the ability to customize decision support rules and their components.	167
					5. The system **SHOULD** provide the ability to inactivate, obsolete, or destroy decision support rules.	168
					6. The system **SHOULD** conform to function IN.2.2 (Auditable Records) to audit all changes to decision support rules.	169
					7. The system **SHOULD** provide the ability to create diagnostic support rules to guide system behavior.	170
					8. The system **SHOULD** provide the ability to update diagnostic support rules.	171
					9. The system **MAY** provide the ability to customize diagnostic support rules and their components.	172
					10. The system **SHOULD** provide the ability to inactivate, obsolete, or destroy diagnostic support rules.	173
					11. The system **SHOULD** conform to function IN.2.2 (Auditable Records) to audit all changes to diagnostic support rules.	174
					12. The system **SHOULD** provide the ability to create workflow control rules to guide system behavior.	175
					13. The system **SHOULD** provide the ability to update workflow control rules.	176
					14. The system **MAY** provide the ability to customize workflow control rules and their components.	177

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			- Classifying a pregnant patient as high risk due to factors such as age, health status, and prior pregnancy outcomes; - Sending an update to an immunization registry when a vaccination is administered; - Limiting access to mental health information to authorized providers; - Establishing system level defaults such as for vocabulary data sets to be implemented.; and - Establishing user level preferences such as allowing the use of health information for research purposes.		15. The system **SHOULD** provide the ability to inactivate, obsolete, or destroy workflow control rules.	178
					16. The system **SHOULD** conform to function IN.2.2 (Auditable Records) to audit all changes to workflow control rules.	179
					17. The system **MAY** provide the ability to create access privilege rules to guide system behavior.	180
					18. The system **MAY** provide the ability to update access privilege rules.	181
					19. The system **MAY** provide the ability to customize access privilege rules and their components.	182
					20. The system **MAY** provide the ability to inactivate, obsolete, or destroy access privilege rules.	183
					21. The system **MAY** conform to function IN.2.2 (Auditable Records) to audit all changes to access privilege rules.	184
					22. The system **SHOULD** conform to function IN.2.2 (Auditable Records) to audit all changes to other business rules.	185
					23. The system **SHOULD** support the ability to selectively export business rules.	186
IN.7	**F**	Workflow Management	**Statement:** Support workflow management functions including both the management and set up of work queues, personnel lists, and system interfaces as well as the implementation functions that use workflow-related business rules to direct the flow of work assignments. **Description:** Workflow management functions that an EHR-S supports include: -Distribution of information to and from internal and external parties; -Support for task-management as well as parallel and serial task distribution; -Support for notification and task routing based on system triggers; and -Support for task assignments, escalations and redirection in		1. The system **SHOULD** use workflow-related business rules to direct the flow of work assignments.	187
					2. The system **SHOULD** provide the ability to create workflow (task list) queues.	188
					3. The system **SHOULD** provide the ability to manage workflow (task list) queues.	189
					4. The system **MAY** provide the ability to manage human resources (i.e., personnel lists) for workflow queues.	190
					5. The system **MAY** use system interfaces that support the management of human resources (i.e., personnel lists).	191
					6. The system **MAY** use system interfaces that support the management of workflow (task lists) queues.	192
					7. The system **MAY** provide the ability to distribute information to and from internal and external parties.	193
					8. The system **MAY** provide the ability to route notifications and tasks based on system triggers.	194
					9. The system **MAY** dynamically escalate workflow according to business rules.	195

ID#	Type	Name	Statement/Description	See Also	Conformance Criteria	Row #
			accordance with business rules. Workflow definitions and management may be implemented by a designated application or distributed across an EHR-S.		10. The system **MAY** dynamically redirect workflow according to business rules.	196
					11. The system **MAY** dynamically reassign workflow according to business rules.	197